

Bruselj, 17. junij 2022
(OR. en)

10396/22

**Medinstitucionalna zadeva:
2021/0224(NLE)**

**SCH-EVAL 83
DATAPROTECT 197
COMIX 324**

IZID POSVETOVANJA

Pošiljatelj:	Generalni sekretariat Sveta
Datum:	17. junij 2022
Prejemnik:	delegacije
Št. predh. dok.:	7788/22
Zadeva:	Izvedbeni sklep Sveta o priporočilu za odpravo pomanjkljivosti, ugotovljenih leta 2020 med ocenjevanjem uporabe schengenskega pravnega reda pri varstvu podatkov v Avstriji

V prilogi vam pošiljamo Izvedbeni sklep Sveta o priporočilu za odpravo pomanjkljivosti, ugotovljenih leta 2020 med ocenjevanjem uporabe schengenskega pravnega reda na področju varstva podatkov v Avstriji, ki ga je Svet sprejel na seji 17. junija 2022.

V skladu s členom 15(3) Uredbe Sveta (EU) št. 1053/2013 z dne 7. oktobra 2013 bo to priporočilo poslano Evropskemu parlamentu in nacionalnim parlamentom.

Izvedbeni sklep Sveta o

PRIPOROČILU

za odpravo pomanjkljivosti, ugotovljenih leta 2020 med ocenjevanjem uporabe schengenskega pravnega reda na področju varstva podatkov v Avstriji

SVET EVROPSKE UNIJE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe Sveta (EU) št. 1053/2013 z dne 7. oktobra 2013 o vzpostavitvi ocenjevalnega in spremljevalnega mehanizma za preverjanje uporabe schengenskega pravnega reda in razveljavitvi Sklepa Izvršnega odbora z dne 16. septembra 1998 o ustanovitvi stalnega odbora o ocenjevanju in izvajanju Schengenskega sporazuma¹ ter zlasti člena 15 Uredbe,

ob upoštevanju predloga Evropske komisije,

ob upoštevanju naslednjega:

- (1) Novembra 2020 je bilo za Avstrijo opravljeno schengensko ocenjevanje na področju varstva podatkov. Po ocenjevanju je bilo z Izvedbenim sklepom Komisije C(2021) 9200 sprejeto poročilo z ugotovitvami in ocenami, v katerem so navedene dobre prakse in pomanjkljivosti, ugotovljene med ocenjevanjem.

¹ UL L 295, 6.11.2013, str. 27.

- (2) Za dobre prakse se šteje zlasti naslednje: da se je osebje avstrijskega organa za varstvo podatkov od zadnjega ocenjevanja že in se bo še povečalo ter da se je povečal proračun; da dogovori med upravljavcem in obdelovalcem podatkov v zvezi s podatki v VIS zagotavljajo, da je raven varstva podatkov visoka in da imajo vse strani, ki sodelujejo v obdelavi podatkov v VIS, vzpostavljene ustrezne zaščitne ukrepe za varstvo podatkov; usposabljanje osebja o zadevah v zvezi z varstvom podatkov glede VIS, ki ga pripravljata ministrstvo za notranje zadeve ter ministrstvo za evropske in mednarodne zadeve; kompleksen pristop ministrstva za evropske in mednarodne zadeve k reviziji vizumskega postopka; da so informacije, ki jih zagotavlja organ za varstvo podatkov v zvezi s SIS II in VIS, zelo izčrpne in lahko dostopne; informacijske mape o SIS in VIS na spletni strani ministrstva za notranje zadeve in to, da ministrstvo za notranje zadeve v kratkem času odgovori na zahteve za dostop v zvezi s SIS II ali VIS.
- (3) Treba bi bilo podati priporočila za ukrepe, ki bi jih morala Avstrija sprejeti za odpravo pomanjkljivosti, ugotovljenih pri ocenjevanju. Glede na pomen spoštovanja schengenskega pravnega reda o varstvu osebnih podatkov bi bilo treba prednost dati izvajanju priporočil 1, 6, 7 in 13, kakor so določena v tem sklepu.
- (4) Ta sklep bi bilo treba poslati Evropskemu parlamentu in nacionalnim parlamentom držav članic. Avstrija bi morala v skladu s členom 16(1) Uredbe (EU) št. 1053/2013 v treh mesecih od sprejetja sklepa pripraviti akcijski načrt, ki obravnava vsa priporočila za odpravo pomanjkljivosti, ugotovljenih v ocenjevalnem poročilu, ter ga predložiti Komisiji in Svetu –

PRIPOROČA:

Avstrija bi morala:

Zakonodaja

1. izvajati člen 79 splošne uredbe o varstvu podatkov (GDPR)¹ in prenesti člen 54 Direktive (EU) 2016/680² v avstrijsko nacionalno zakonodajo, da se zagotovi pravica do učinkovitega pravnega sredstva zoper odločitev upravljavca ali obdelovalca, ki je javni organ;

Organ za varstvo podatkov

2. v zakonodaji določiti razloge za razrešitev vodje in namestnika vodje avstrijskega organa za varstvo podatkov, da se prepreči tveganje predčasnega prenehanja njunega mandata, razen v primeru hujše kršitve ali če prenehata izpolnjevati pogoje za opravljanje nalog;
3. zagotoviti, da strokovnjak za informacijsko tehnologijo, na novo zaposlen na organu za varstvo podatkov, pa tudi kateri koli dodatni strokovnjak za informacijsko tehnologijo, ima ali osvoji celovito razumevanje Schengenskega informacijskega sistema II ter upravljanja varnosti informacij, tako da bodo taki strokovnjaki lahko tudi dejavno vključeni v nadzorne dejavnosti v zvezi s SIS in VIS. Nadalje bi moral organ za varstvo podatkov, dokler inšpekcijskih pregledov v zvezi z informacijsko tehnologijo ne more pokriti z lastnim osebjem, v take preglede še naprej vključevati zunanje strokovnjake za informacijsko tehnologijo;

¹ Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1).

² Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ (UL L 119, 4.5.2016, str.89).

4. zagotoviti, da organ za varstvo podatkov opravi inšpekcijske obiske v uradu SIRENE, inšpekcijske preglede nekaterih organov, ki so končni uporabniki sistema, na primer policije, ter redne kontrole in analize dnevniških datotek, da izpolni svoje naloge celovitega spremljanja obdelave osebnih podatkov v SIS II;
5. zagotoviti, da nadzorne dejavnosti organa za varstvo podatkov v zvezi z VIS zajemajo tudi vse varnostne vidike, vključno z dnevniškimi datotekami, in sicer z rednimi kontrolami na podlagi analize dnevniških datotek, ter da organ za varstvo podatkov temeljito pregleda strežniške sobe in tudi nekatere končne uporabnike sistema VIS, na primer policijo;
6. zagotoviti, da organ za varstvo podatkov zaključi drugo revizijo N. VIS, čim bodo razmere v zvezi s COVID-19 to dovoljevale;
7. zagotoviti, da organ za varstvo podatkov vsaj enkrat na štiri leta opravi revizijo postopkov obdelave podatkov v N. VIS;

Schengenski informacijski sistem

8. zagotoviti, da se na vseh napravah, ki omogočajo dostop do podatkov v SIS II, uporablja dvofaktorska avtentikacija;
9. zagotoviti, da se vsi dokumenti sistemov upravljanja informacijske varnosti, ki se uporabljajo za oba podatkovna centra, pogosteje pregledujejo in da se še naprej uporabljajo najvišji standardi;
10. zagotoviti, da se varnostni načrt za SIS II redno pregleduje in po potrebi posodablja ter da se določijo varnostni ukrepi, ki bodo poleg zaupnosti, integritete in dostopnosti zagotavljali trajno odpornost, zlasti z zagotavljanjem, da upravljavec upošteva tehnični razvoj in tako zagotovi nadaljnjo ustreznost sprejetih varnostnih ukrepov;

11. pojasniti, ali je osrednji organ za potrdila o nekaznovanosti sestavni del ministrstva za notranje zadeve ali zunanjega obdelovalca podatkov;
12. zagotoviti, da se za upravljanje zadev v zvezi z zlorabo identitete izboljšajo informacije, ki se dajo posameznikom, na katere se nanašajo osebni podatki, in obrazci za privolitev ter da obrazci, ki se dajo posameznikom, na katere se nanašajo osebni podatki, navajajo informacije o pravicah teh posameznikov, kontaktne podatke pooblaščenih oseb za varstvo podatkov, pravno podlago in trajanju hrambe osebnih podatkov;

Vizumski informacijski sistem

13. zagotoviti, da se v skladu s členom 34 Uredbe (ES) št. 767/2008 (Uredba VIS) na nacionalni ravni vodijo dnevniki o vseh postopkih obdelave podatkov v VIS (za čas enega leta po obdobju hrambe iz člena 23(1) Uredbe VIS);

Ozaveščenost javnosti in pravice posameznikov, na katere se nanašajo podatki

14. zagotoviti, da ministrstvo za notranje zadeve poleg nemške zagotovi tudi druge jezikovne različice – na primer angleško – svoje spletne strani o obdelavi podatkov v SIS II in VIS ter o povezanih pravicah posameznikov, na katere se nanašajo podatki, ter da zagotovi lažji dostop do informacij o pravicah posameznikov, na katere se nanašajo osebni podatki, v zvezi s SIS II in VIS, na svoji spletni strani;
15. zagotoviti, da ministrstvo za notranje zadeve na svoji spletni strani zagotovi obrazce za uveljavljanje pravice do dostopa, popravka in izbrisa, in sicer v nemščini in drugih jezikih, na primer v angleščini;
16. poskrbeti, da bodo papirnate različice informativnih brošur o SIS na voljo in dostopne v javnih organih;

17. z namenom krepitev pravic posameznikov, na katere se nanašajo osebni podatki, zagotoviti, da ministrstvo za notranje zadeve poskrbi za neuradni prevod odgovorov posameznikom, na katere se nanašajo osebni podatki, na primer v angleščino;
18. zagotoviti, da so na spletnih straneh policijskih uprav zveznih dežel objavljene informacije o SIS II in VIS, med drugim o povezani obdelavi osebnih podatkov, ter povezave na spletno stran organa za varstvo podatkov;
19. zagotoviti, da so informacije o obdelavi osebnih podatkov v VIS lahko dostopne na spletnih straneh ministrstva za evropske in mednarodne zadeve ter konzulatov in veleposlaništev ter da te spletne strani vsebujejo povezave na spletno stran organa za varstvo podatkov;
20. zagotoviti, da organ za varstvo podatkov na svoji spletni strani (v nemščini in angleščini) in v obrazcih za zahtevo za dostop zagotovi enake informacije o obveznosti posameznika, na katerega se nanašajo osebni podatki, da dokaže svojo identiteto;
21. zagotoviti, da organ za varstvo podatkov na svoji spletni strani (v nemščini in angleščini) zagotovi posebne standardne obrazce za zahteve za popravke in izbris v zvezi s podatki v VIS in SIS;
22. zagotoviti, da organ za varstvo podatkov zagotovi informacije o roku za vložitev pritožbe, kakor je določeno v členu 24(4) zakona o varstvu podatkov, na angleški različici svoje spletne strani.

V Bruslju,

Za Svet
predsednik/predsednica